



0400
5-22-01

0700
5-2-01

PATENT
81754.0056

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Eriko GOTO et al.

Serial No: 09/821,729

Filed: March 28, 2001

For: NETWORK SECURITY SYSTEM

Art Unit: Not assigned

Examiner: Not assigned

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:

Assistant Commissioner for Patents
Washington D.C. 20231, on

April 24, 2001

Date of Deposit

Michael Crapenhof, Reg. No. 37,115

Name

Michael Crapenhof 4/24/01

Signature

Date

TRANSMITTAL OF PRIORITY DOCUMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-092496 which was filed March 29, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: April 24, 2001

By:

Michael Crapenhof
Michael Crapenhof
Registration No. 37,115
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

09/821729



日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

2000年 3月29日

出 願 番 号
Application Number:

特願2000-092496

願 人
Applicant (s):

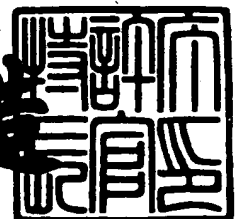
セイコーエプソン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 4月13日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3030092

【書類名】 特許願

【整理番号】 J0077734

【提出日】 平成12年 3月29日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00

【発明者】

 【住所又は居所】 長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

 【氏名】 後藤 恵理子

【発明者】

 【住所又は居所】 長野県諏訪市大和3丁目3番5号 エプソンダイレクト株式会社内

 【氏名】 渋谷 泰夫

【発明者】

 【住所又は居所】 長野県諏訪市大和3丁目3番5号 エプソンダイレクト株式会社内

 【氏名】 大島 康弘

【特許出願人】

 【識別番号】 000002369

 【氏名又は名称】 セイコーエプソン株式会社

 【代表者】 安川 英昭

【代理人】

 【識別番号】 100093388

 【弁理士】

 【氏名又は名称】 鈴木 喜三郎

 【連絡先】 0 2 6 6 - 5 2 - 3 1 3 9

【選任した代理人】

 【識別番号】 100095728

 【弁理士】

【氏名又は名称】 上柳 雅誉

【選任した代理人】

【識別番号】 100107261

【弁理士】

【氏名又は名称】 須澤 修

【手数料の表示】

【予納台帳番号】 013044

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9711684

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークセキュリティシステム

【特許請求の範囲】

【請求項 1】 ネットワークに接続されたサーバと、

前記ネットワークを通じてサーバが受信した外部形式のデータを記憶する受信データ記憶手段と、

この受信データ記憶手段に記憶された外部形式のデータを、内部形式のデータに変換して、受信処理データ記憶手段に記憶させる受信データ形式変換手段と、

前記受信処理データ記憶手段に記憶された内部形式のデータを利用して所定の処理を実行するホストコンピュータとを備えたことを特徴とするネットワークセキュリティシステム。

【請求項 2】 請求項 1 に記載のネットワークセキュリティシステムにおいて、

受信データ記憶手段は、サーバが受信した外部形式のデータの書き込みを許容し、かつ、サーバによるデータの読み出しを禁止し、受信処理データ記憶手段は、ホストコンピュータによる内部形式のデータの読み出しを許容し、かつ、ホストコンピュータによるデータの書き込みを禁止することを特徴とするネットワークセキュリティシステム。

【請求項 3】 請求項 1 または 2 に記載のネットワークセキュリティシステムにおいて、

受信データ記憶手段は、受信データ形式変換手段による外部形式のデータの読み出しを許容し、かつ、受信データ形式変換手段によるデータの書き込みを禁止し、受信処理データ記憶手段は、受信データ形式変換手段による内部形式のデータの書き込みを許容し、かつ、受信データ形式変換手段によるデータの読み出しを禁止することを特徴とするネットワークセキュリティシステム。

【請求項 4】 請求項 1 乃至 3 のいずれかに記載のネットワークセキュリティシステムにおいて、

前記内部形式のデータは、受信処理データ記憶手段からホストコンピュータ側のデータベースに所定のタイミングで追加記憶されることを特徴とするネットワークセキュリティシステム。

【請求項 5】 請求項 4 に記載のネットワークセキュリティシステムにおいて、
前記受信データ形式変換手段による外部形式のデータから内部形式のデータへの変換処理と、前記内部形式のデータのホストコンピュータ側のデータベースへの追加記憶処理はそれぞれ独自のタイミングで一括して実行されることを特徴とするネットワークセキュリティシステム。

【請求項 6】 請求項 1 乃至 3 のいずれかに記載のネットワークセキュリティシステムにおいて、

受信データ形式変換手段は、外部形式のデータをデータベース形式のデータに変換することを特徴とするネットワークセキュリティシステム。

【請求項 7】 請求項 1 乃至 3 のいずれかに記載のネットワークセキュリティシステムにおいて、

サーバは受信データ記憶手段にメール形式のデータを送信して外部形式のデータを書き込むことを特徴とするネットワークセキュリティシステム。

【請求項 8】 請求項 1 乃至 3 のいずれかに記載のネットワークセキュリティシステムにおいて、

前記ネットワークはインターネットであることを特徴とするネットワークセキュリティシステム。

【請求項 9】 内部形式のデータを利用して所定の処理を実行するホストコンピュータと、

ネットワークに送信される内部形式のデータを記憶する送信処理データ記憶手段と、

この送信処理データ記憶手段に記憶された内部形式のデータを外部形式のデータに変換して、送信データ記憶手段に記憶させる送信データ形式変換手段と、

前記送信データ記憶手段に記憶された外部形式のデータをネットワークに対して送信するサーバとを備えたことを特徴とするネットワークセキュリティシステム。

【請求項 10】 請求項 9 に記載のネットワークセキュリティシステムにおいて

送信処理データ記憶手段は、ホストコンピュータによる内部形式のデータの書

き込みを許容し、かつ、ホストコンピュータによるデータの読み出しを禁止して、送信データ記憶手段は、サーバが送信する外部形式のデータの読み出しを許容し、かつ、サーバによるデータの書き込みを禁止することを特徴とするネットワークセキュリティシステム。

【請求項 1 1】 請求項 9 または 1 0 に記載のネットワークセキュリティシステムにおいて、

送信処理データ記憶手段は、送信データ形式変換手段による内部形式のデータの読み出しを許容し、かつ、送信データ形式変換手段によるデータの書き込みを禁止し、送信データ記憶手段は、送信データ形式変換手段による外部形式のデータの書き込みを許容し、かつ、送信データ形式変換手段によるデータの読み出しを禁止することを特徴とするネットワークセキュリティシステム。

【請求項 1 2】 請求項 9 乃至 1 1 のいずれかに記載のネットワークセキュリティシステムにおいて、

前記送信データ形式変換手段による内部形式のデータから外部形式のデータへの変換処理は、前記ホストコンピュータによる送信処理データ記憶手段への内部形式のデータの記憶処理とは独立したタイミングで実行されることを特徴とするネットワークセキュリティシステム。

【請求項 1 3】 請求項 9 乃至 1 1 のいずれかに記載のネットワークセキュリティシステムにおいて、

サーバは送信データ記憶手段からメール形式のデータを受信してネットワークに送信することを特徴とするネットワークセキュリティシステム。

【請求項 1 4】 請求項 9 乃至 1 1 のいずれかに記載のネットワークセキュリティシステムにおいて、

前記ネットワークはインターネットであることを特徴とするネットワークセキュリティシステム。

【請求項 1 5】 ネットワークを通じてサーバが受信した外部形式のデータを記憶する受信データ記憶手段と、

この受信データ記憶手段に記憶された外部形式のデータを、内部形式のデータに変換して、受信処理データ記憶手段に記憶させる受信データ形式変換手段と、

前記受信処理データ記憶手段に記憶された内部形式のデータを利用して所定の処理を実行するホストコンピュータと、

ネットワークに送信される内部形式のデータを記憶する送信処理データ記憶手段と、

この送信処理データ記憶手段に記憶された内部形式のデータを外部形式のデータに変換して、送信データ記憶手段に記憶させる送信データ形式変換手段と、

前記送信データ記憶手段に記憶された外部形式のデータをネットワークに対して送信するサーバとを備えたことを特徴とするネットワークセキュリティシステム。

【請求項 1 6】 請求項 1 5 に記載のネットワークセキュリティシステムにおいて、

前記受信データ形式変換手段による外部形式のデータから内部形式のデータへの変換処理と、

前記内部形式のデータのホストコンピュータ側のデータベースへの追加記憶処理と、

前記送信データ形式変換手段による内部形式のデータから外部形式のデータへの変換処理と、

前記ホストコンピュータによる送信処理データ記憶手段への内部形式のデータの記憶処理とは、

それぞれ独立したタイミングで実行されることを特徴とするネットワークセキュリティシステム。

【請求項 1 7】 ネットワークに接続されたサーバと、ホストコンピュータ側に接続されたメール転送部とから成り、

前記サーバにはメールクライアントとメールサーバとが設けられ、

前記メール転送部には、前記メールクライアントから通信回線を介してメールを受信するメール受信部と、前記メールサーバに通信回線を介してメールを送信するメール送信部とが設けられ、

前記ホストコンピュータは前記メール転送部のメール受信部を介して前記サーバからデータの転送を受け、前記メール転送部のメール送信部を介して前記サ

バにデータを転送することを特徴とするネットワークセキュリティシステム。

【請求項 1 8】 請求項 1 7 に記載のネットワークセキュリティシステムにおいて、

前記通信回線は、メール専用の通信回線であることを特徴とするネットワークセキュリティシステム。

【請求項 1 9】 ネットワークに側に設けたメールサーバと、

ホストコンピュータ側に設けられたメール転送部とから成り、

前記メール転送部には、前記メールサーバからメール専用線を介してメールを受信するメール受信部と、前記メールサーバにメール専用線を介してメールを送信するメール送信部とが設けられ、

前記ホストコンピュータは前記メール転送部のメール受信部を介して前記メールサーバからデータの転送を受け、前記メール転送部のメール送信部を介して前記メールサーバにデータを転送することを特徴とするネットワークセキュリティシステム。

ネットワーク側にメールサーバを配置して、このメールサーバとホストコンピュータ側のメール転送部との間のメール送受信を専用線を介して行う。専用線は、通信線であればなんでもよいが、メールサーバとホストコンピュータ側の通信にのみ使用される。専用線により一定の手段によってのみネットワークとホストコンピュータとの間のデータ転送をするので、ホストコンピュータ側がネットワーク側から保護される。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、ネットワークを通じてデータの送受信をする内部システムを、ネットワークから保護するネットワークセキュリティシステムに関する。

【0 0 0 2】

【従来技術】

インターネット等のネットワークを利用して商品の販売等を行うシステムでは、ネットワークを通じて受注情報を取得し、この受注情報をデータベースに書き

込んで、商品の手配や発送等の管理を行っている。このようなシステムでは、万一、ネットワークから不正なデータを取り込んで受注情報が破壊されると、受注活動が停止して重大な被害が発生する。また、万一、不正な手段でネットワークを通じて顧客情報が読みだされると、深刻な信用上の問題が発生する。そこで、いわゆるファイヤーウォールと呼ばれる保護システムをネットワークと内部システムとの間に設けることによって、ハッカー等の侵入を阻止するようにしている。

【 0 0 0 3 】

【発明が解決しようとする課題】

ところで、上記のような従来の技術には、次のような解決すべき課題があった。

ファイヤーウォールは、ネットワークを通じて内部システムにアクセスしようとする相手方のアクセス権を確認するために、識別情報や暗証コードなどを要求し、その認証を行なう（特開平 1 1 - 2 9 8 6 3 9 号公報、特開平 1 0 - 2 1 4 3 0 4 号公報）。ところが、不正な手段で識別情報や暗証コードを入手して偽装するハッカーに対する防御は容易でない。しかも、商品の受注販売システムのように、不特定多数のユーザから受注情報を受け入れてこれをデータベースに取り込むものでは、受注情報に混じって侵入する不正なデータを的確に排除する機構が要求される。また、データベースの内容を不正に読みだす行為を的確に排除する機構が要求される。

【 0 0 0 4 】

【課題を解決するための手段】

本発明は以上の点を解決するため次の構成を採用する。

【 0 0 0 5 】

〈構成 1〉

ネットワークに接続されたサーバと、上記ネットワークを通じてサーバが受信した外部形式のデータを記憶する受信データ記憶手段と、この受信データ記憶手段に記憶された外部形式のデータを、内部形式のデータに変換して、受信処理データ記憶手段に記憶させる受信データ形式変換手段と、上記受信処理データ記憶

手段に記憶された内部形式のデータを利用して所定の処理を実行するホストコンピュータとを備えたことを特徴とするネットワークセキュリティシステム。

【 0 0 0 6 】

サーバはネットワークに接続されている。外部形式のデータはネットワークを通じて他の端末装置等から受信される。外部形式のデータのデータ形式は任意でよい。内部形式のデータのデータ形式も任意である。受信データ形式変換手段は、受信データ記憶手段から外部形式のデータを読み取って、所定の手順で内部形式のデータに変換した後、受信処理データ記憶手段に書き込む。受信処理データ記憶手段に記憶された内部形式のデータはホストコンピュータに利用される。受信データ形式変換手段は、外部形式のデータから必要なデータのみを抽出加工して、予め定めた安全な内部形式のデータに変換をする役割を持つ。

【 0 0 0 7 】

ネットワークを通じて受信した外部形式のデータは受信データ記憶手段に書き込まれるが、ホストコンピュータはこの受信データ記憶手段を直接アクセスしない。故に、不正なデータの取り込みが防止できる。即ち、受信データ形式変換手段が外部形式のデータを内部形式のデータに変換する際に、外部形式のデータを安全な内部形式のデータに変換することができるので、不正なデータを排除できる。ホストコンピュータは、任意のタイミングで受信処理データ記憶手段をアクセスして、内部形式のデータを利用すればよい。

【 0 0 0 8 】

〈構成 2〉

構成 1 に記載のネットワークセキュリティシステムにおいて、受信データ記憶手段は、サーバが受信した外部形式のデータの書き込みを許容し、かつ、サーバによるデータの読み出しを禁止し、受信処理データ記憶手段は、ホストコンピュータによる内部形式のデータの読み出しを許容し、かつ、ホストコンピュータによるデータの書き込みを禁止することを特徴とするネットワークセキュリティシステム。

【 0 0 0 9 】

受信データ記憶手段がサーバによるデータの読み出しを禁止するのは、ネット

ワーク側から受信データ記憶手段中のデータの読み出しがされるのを防止するためである。ホストコンピュータによる受信処理データ記憶手段へのデータの書き込みを禁止するのは、ホストコンピュータ側から不用意にデータがネットワーク側に出力されるのを防止するためである。これにより、ホストコンピュータ側からネットワーク側へのデータの流れが禁止されて、ホストコンピュータ側のデータがネットワーク側に読み出されることが無い。なお、書き込みや読み出しを禁止されるのは全てのデータが対象になり、内部形式のデータも外部形式のデータも別の形式のデータも含む。

【 0 0 1 0 】

〈構成 3〉

構成 1 または 2 に記載のネットワークセキュリティシステムにおいて、受信データ記憶手段は、受信データ形式変換手段による外部形式のデータの読み出しを許容し、かつ、受信データ形式変換手段によるデータの書き込みを禁止し、受信処理データ記憶手段は、受信データ形式変換手段による内部形式のデータの書き込みを許容し、かつ、受信データ形式変換手段によるデータの読み出しを禁止することを特徴とするネットワークセキュリティシステム。

【 0 0 1 1 】

受信データ形式変換手段は、受信データ記憶手段から外部形式のデータの読み出しのみが許容され、受信処理データ記憶手段への内部形式のデータの書き込みのみが許容される。こうして、受信データ形式変換手段によるデータの流れを、ネットワーク側からホストコンピュータ側への一方通行にしている。これにより、ホストコンピュータ側からネットワーク側へのデータの流れを禁止して、ホストコンピュータ側のデータを保護できる。

【 0 0 1 2 】

〈構成 4〉

構成 1 乃至 3 のいずれかに記載のネットワークセキュリティシステムにおいて、上記内部形式のデータは、受信処理データ記憶手段からホストコンピュータ側のデータベースに所定のタイミングで追加記憶されることを特徴とするネットワークセキュリティシステム。

【 0 0 1 3 】

受信処理データ記憶手段がホストコンピュータとは別に設けられている場合には、受信処理データ記憶手段からホストコンピュータ側のデータベースに該当するデータが転送される。受信データ形式変換手段の動作等とは独立した所定のタイミングでデータを転送することができる。ホストコンピュータ側のデータベースのアップデートのタイミングは任意である。

【 0 0 1 4 】

〈構成 5〉

構成 4 に記載のネットワークセキュリティシステムにおいて、上記受信データ形式変換手段による外部形式のデータから内部形式のデータへの変換処理と、上記内部形式のデータのホストコンピュータ側のデータベースへの追加記憶処理はそれぞれ独自のタイミングで一括して実行されることを特徴とするネットワークセキュリティシステム。

【 0 0 1 5 】

サーバが受信データ記憶手段に受信データを書き込むのは、通常、1 個のデータごとになる。しかし、受信データ形式変換手段は、変換処理を一括して実行する。一括して実行するというのは、1 個のデータごとではなく、バッチ処理のように複数のデータをまとめて処理するという意味である。独自のタイミングで実行されるというのは、それぞれ起動制御が独立しているという意味である。もちろん、例えば、受信データ形式変換手段の変換処理が終了すると自動的に、ホストコンピュータ側のデータベースへの追加記憶処理が開始するように、動作タイミングを制御してもかまわない。

【 0 0 1 6 】

〈構成 6〉

構成 1 乃至 3 のいずれかに記載のネットワークセキュリティシステムにおいて、受信データ形式変換手段は、外部形式のデータをデータベース形式のデータに変換することを特徴とするネットワークセキュリティシステム。

【 0 0 1 7 】

ネットワークから受信したデータをホストコンピュータで処理するデータベ

スに取り込むために、必要な変換処理だけを行う。従って、不正なデータがホストコンピュータ側に取り込まれるのを防止できる。

【 0 0 1 8 】

〈構成 7〉

構成 1 乃至 3 のいずれかに記載のネットワークセキュリティシステムにおいて、サーバは受信データ記憶手段にメール形式のデータを送信して外部形式のデータを書き込むことを特徴とするネットワークセキュリティシステム。

【 0 0 1 9 】

サーバが一般の記憶装置上の記憶領域をアクセスして外部形式のデータを書き込むようにするよりも、サーバから受信データ記憶手段にメール形式のデータを送信するようにしたほうが、サーバから受信データ記憶手段へのデータの一方通行性が確保される。

【 0 0 2 0 】

〈構成 8〉

構成 1 乃至 3 のいずれかに記載のネットワークセキュリティシステムにおいて、上記ネットワークはインターネットであることを特徴とするネットワークセキュリティシステム。

【 0 0 2 1 】

イントラネットに比べてはるかに高いセキュリティが要求されるからこのシステムを採用した。

【 0 0 2 2 】

〈構成 9〉

内部形式のデータを利用して所定の処理を実行するホストコンピュータと、ネットワークに送信される内部形式のデータを記憶する送信処理データ記憶手段と、この送信処理データ記憶手段に記憶された内部形式のデータを外部形式のデータに変換して、送信データ記憶手段に記憶させる送信データ形式変換手段と、上記送信データ記憶手段に記憶された外部形式のデータをネットワークに対して送信するサーバとを備えたことを特徴とするネットワークセキュリティシステム。

【 0 0 2 3 】

サーバはネットワークに接続されている。外部形式のデータはネットワークを通じて他の端末装置等に送信される。外部形式のデータやデータ形式、内部形式のデータやデータ形式、データ形式の変換の内容はデータ受信の場合と変わらない。送信データ形式変換手段は、送信処理データ記憶手段から内部形式のデータを読み取って、所定の手順で外部形式のデータに変換した後、送信データ記憶手段に書き込む。

【 0 0 2 4 】

ホストコンピュータは、任意のタイミングで送信処理データ記憶手段に、送信すべき内部形式のデータを書き込む。サーバによりネットワークを通じて送信される外部形式のデータは、送信データ形式変換手段により送信データ記憶手段に書き込まれる。サーバは、送信処理データ記憶手段を直接アクセスしない。故に、誤って、ホストコンピュータ側の保護すべきデータの送信がされるのを防止できる。

【 0 0 2 5 】

〈構成 1 0〉

構成 9 に記載のネットワークセキュリティシステムにおいて、送信処理データ記憶手段は、ホストコンピュータによる内部形式のデータの書き込みを許容し、かつ、ホストコンピュータによるデータの読み出しを禁止して、送信データ記憶手段は、サーバが送信する外部形式のデータの読み出しを許容し、かつ、サーバによるデータの書き込みを禁止することを特徴とするネットワークセキュリティシステム。

【 0 0 2 6 】

送信処理データ記憶手段がホストコンピュータによるデータの読み出しを禁止するのは、ネットワーク側から不正なデータが侵入するのを防止するためである。サーバによる送信データ記憶手段へのデータの書き込みを禁止するのも、ネットワーク側から不正なデータが侵入するのを防止するためである。これにより、ホストコンピュータ側からネットワーク側へのデータの流れのみが確保されて、ホストコンピュータを含む内部システムが保護される。なお、書き込みや読み出しを禁止されるのは全てのデータが対象になり、その形式は問わない。

【 0 0 2 7 】

〈構成 1 1〉

構成 9 または 1 0 に記載のネットワークセキュリティシステムにおいて、送信処理データ記憶手段は、送信データ形式変換手段による内部形式のデータの読み出しを許容し、かつ、送信データ形式変換手段によるデータの書き込みを禁止し、送信データ記憶手段は、送信データ形式変換手段による外部形式のデータの書き込みを許容し、かつ、送信データ形式変換手段によるデータの読み出しを禁止することを特徴とするネットワークセキュリティシステム。

【 0 0 2 8 】

送信データ形式変換手段は、送信処理データ記憶手段から内部形式のデータの読み出しのみが許容され、送信処理データ記憶手段への外部形式のデータの書き込みのみが許容される。こうして、送信データ形式変換手段によるデータの流れを、ホストコンピュータ側からネットワーク側への一方通行にしている。これにより、ネットワーク側からホストコンピュータ側へのデータの流れを禁止して、ホストコンピュータ側のデータを保護できる。

【 0 0 2 9 】

〈構成 1 2〉

構成 9 乃至 1 1 のいずれかに記載のネットワークセキュリティシステムにおいて、上記送信データ形式変換手段による内部形式のデータから外部形式のデータへの変換処理は、上記ホストコンピュータによる送信処理データ記憶手段への内部形式のデータの記憶処理とは独立したタイミングで実行されることを特徴とするネットワークセキュリティシステム。

【 0 0 3 0 】

送信処理データ記憶手段を設けているので、送信データ形式変換手段は、変換処理を任意のタイミングで実行できる。また、ホストコンピュータも任意のタイミングで送信用の内部形式のデータを送信処理データ記憶手段へ書き込むことができる。送信用の内部データの形式は自由で、データベース用とは限らない。

【 0 0 3 1 】

〈構成 1 3〉

構成 9 乃至 1 1 のいずれかに記載のネットワークセキュリティシステムにおいて、サーバは送信データ記憶手段からメール形式のデータを受信してネットワークに送信することを特徴とするネットワークセキュリティシステム。

【 0 0 3 2 】

サーバが一般の記憶装置上の記憶領域をアクセスして外部形式のデータを書き込むようにするよりも、サーバが送信データ記憶手段からメール形式のデータを受信するようにしたほうが、送信データ記憶手段からサーバへのデータの一方通行性が確保される。

【 0 0 3 3 】

〈構成 1 4〉

構成 9 乃至 1 1 のいずれかに記載のネットワークセキュリティシステムにおいて、上記ネットワークはインターネットであることを特徴とするネットワークセキュリティシステム。

【 0 0 3 4 】

イントラネットに比べてはるかに高いセキュリティが要求されるからこのシステムを採用した。

【 0 0 3 5 】

〈構成 1 5〉

ネットワークを通じてサーバが受信した外部形式のデータを記憶する受信データ記憶手段と、この受信データ記憶手段に記憶された外部形式のデータを、内部形式のデータに変換して、受信処理データ記憶手段に記憶させる受信データ形式変換手段と、上記受信処理データ記憶手段に記憶された内部形式のデータを利用して所定の処理を実行するホストコンピュータと、ネットワークに送信される内部形式のデータを記憶する送信処理データ記憶手段と、この送信処理データ記憶手段に記憶された内部形式のデータを外部形式のデータに変換して、送信データ記憶手段に記憶させる送信データ形式変換手段と、上記送信データ記憶手段に記憶された外部形式のデータをネットワークに対して送信するサーバとを備えたことを特徴とするネットワークセキュリティシステム。

【 0 0 3 6 】

構成1のデータ受信機能と構成9のデータ送信機能の双方を備えたシステムである。

【0037】

〈構成16〉

構成15に記載のネットワークセキュリティシステムにおいて、上記受信データ形式変換手段による外部形式のデータから内部形式のデータへの変換処理と、上記内部形式のデータのホストコンピュータ側のデータベースへの追加記憶処理と、上記送信データ形式変換手段による内部形式のデータから外部形式のデータへの変換処理と、上記ホストコンピュータによる送信処理データ記憶手段への内部形式のデータの記憶処理とは、それぞれ独立したタイミングで実行されることを特徴とするネットワークセキュリティシステム。

【0038】

このように一方通行の障壁を設け、かつ、それぞれ独自のタイミングで順次データ転送を行うようにしているので、ネットワークからのホストコンピュータ側の保護が強固になる。故に、ネットワーク側から構成1のデータ受信機能を利用して所定のコマンドを送り込み、構成9のデータ送信機能を利用してホストコンピュータ側から何らかのデータを読みだすのは不可能になるという効果がある。

【0039】

〈構成17〉

ネットワークに接続されたサーバと、ホストコンピュータ側に接続されたメール転送部とから成り、上記サーバにはメールクライアントとメールサーバとが設けられ、上記メール転送部には、上記メールクライアントから通信回線を介してメールを受信するメール受信部と、上記メールサーバに通信回線を介してメールを送信するメール送信部とが設けられ、上記ホストコンピュータは上記メール転送部のメール受信部を介して上記サーバからデータの転送を受け、上記メール転送部のメール送信部を介して上記サーバにデータを転送することを特徴とするネットワークセキュリティシステム。

【0040】

サーバとメール転送部との間でのデータ転送は、一定のメール形式以外で行わ

れることがない。ホストコンピュータはメール転送部を介してのみ、サーバとデータの授受を行う。故に、不正なコマンドやプログラムがサーバとメール転送部との間で転送されることが無い。

【 0 0 4 1 】

〈構成 1 8〉

構成 1 7 に記載のネットワークセキュリティシステムにおいて、上記通信回線は、メール専用の通信回線であることを特徴とするネットワークセキュリティシステム。

【 0 0 4 2 】

メール専用であって、他のデータの侵入経路を持たない通信回線を用いてサーバとメール転送部とを接続すれば、より確実にセキュリティを保つことができる。

【 0 0 4 3 】

〈構成 1 9〉

ネットワークに側に設けたメールサーバと、ホストコンピュータ側に設けられたメール転送部とから成り、上記メール転送部には、上記メールサーバからメール専用線を介してメールを受信するメール受信部と、上記メールサーバにメール専用線を介してメールを送信するメール送信部とが設けられ、上記ホストコンピュータは上記メール転送部のメール受信部を介して上記メールサーバからデータの転送を受け、上記メール転送部のメール送信部を介して上記メールサーバにデータを転送することを特徴とするネットワークセキュリティシステム。

【 0 0 4 4 】

ネットワーク側にメールサーバを配置して、このメールサーバとホストコンピュータ側のメール転送部との間のメール送受信を専用線を介して行う。専用線は、通信線であればなんでもよいが、メールサーバとホストコンピュータ側の通信にのみ使用される。専用線により一定の手段によってのみネットワークとホストコンピュータとの間のデータ転送をするので、ホストコンピュータ側がネットワーク側から保護される。

【 0 0 4 5 】

【発明の実施の形態】

以下、本発明の実施の形態を具体例を用いて説明する。

【0046】

〈受信処理〉

図1は、本発明のシステムの具体例を示すブロック図である。

図のように、ネットワーク1にはユーザの利用する様々な端末装置2が接続されている。これらの端末装置2に対して、例えば、商品購入の為の情報を提供するシステムが接続されている。このシステムは、本発明により保護機能を強化したネットワークセキュリティシステム20を構成している。ネットワークセキュリティシステム20は、サーバ3、受信データ記憶手段6、受信データ形式変換手段7、受信処理データ記憶手段8及びホストコンピュータ10を備える。

【0047】

サーバ3は、ネットワーク1に接続されている。サーバ3の内部には、ユーザに提供するための情報を記憶した図示しない記憶装置が組み込まれている。なお、このネットワークは、インターネットが適するが、この他に、利用者を特定した電話網、イントラネットその他あらゆるネットワークに適用が可能である。

【0048】

ユーザから商品の受注をしたときには、その受注情報はネットワーク1を通じてサーバ3が受信する。この受注情報を処理して商品の手配や管理を行うために、ホストコンピュータ10が設けられている。受信データ記憶手段6と、受信データ形式変換手段7と、受信処理データ記憶手段8は、サーバが受信した受注情報をホストコンピュータ10に送り込むためのものである。ホストコンピュータ10は、受信処理データ記憶手段8からデータベース記憶部9にその受注情報を受け入れて、受注管理を行う。

【0049】

受信データ記憶手段6は、ネットワークを通じてサーバ3が受信した外部形式のデータ4を記憶する記憶装置により構成される。外部形式のデータ4はネットワークを通じて他の端末装置等から受信されるもので、Eメール形式、データファイル形式等の任意の形式のデータである。また、テキスト形式のデータでもバ

イナリ形式のデータでも構わない。受信データ形式変換手段 7 は、受信データ記憶手段 6 から外部形式のデータ 4 を読み取って、所定の手順で内部形式のデータ 5 に変換した後、受信処理データ記憶手段 8 に書き込む機能を持つ。受信データ形式変換手段 7 は、コンピュータプログラムにより実現するとよいが、ハードウェアにより実現することもできる。データ形式の変換は、抽出、並べ替え、部分的な削除、データの追加等、自由に設定できる。受信データ形式変換手段 7 は、単なるデータの転送をしないので受信データに含まれる不正なデータをフィルタリングする効果がある。

【 0 0 5 0 】

内部形式のデータ 5 の形式も任意であるが、予めホストコンピュータ側で規定された所定のフォーマットのデータである。この例では、データベース記憶部 9 に記憶されたデータベースを容易にアップデートすることができるよう、CSV 形式のデータとする。この CSV 形式のデータは、データが項目毎にカンマやタブで区切られたテキスト形式のデータである。受信データ形式変換手段 7 は、サーバ 3 の受信した外部形式のデータを解析して、必要なデータ項目を抽出し、内部形式のデータを生成する。受信処理データ記憶手段 8 は、この内部形式のデータ 5 を所定量記憶して、データベース記憶部 9 にその内部形式のデータ 5 を書き込む迄保持する記憶装置である。

【 0 0 5 1 】

図 2 は、サーバが受信したデータが変換されて受信処理データ記憶手段に記憶されるまでの動作を説明する説明図である。また、図 3 は、サーバや受信処理データ記憶手段等の動作のフローチャートである。

これらの図を用いて、その動作を説明する。まず、サーバは、図 1 に示したネットワーク 1 から受信したデータ D 1 を順番に受信データ記憶手段 6 に書き込む（図 3 ステップ S 1、ステップ S 2）。受信データ記憶手段 6 に蓄積されたデータ D 2 は、所定のタイミングで受信データ形式変換手段 7 により読み取られ、外部形式のデータ 4 から内部形式のデータ 5 への変換処理が行われる（図 3 ステップ S 3、ステップ S 4）。

【 0 0 5 2 】

例えば、受注データ管理の場合には、こうした変換処理は、毎日夜間に1回とか、1日2回とか、2時間置きといったように設定される。従って、受信データ形式変換手段7はシステムタイマを監視して、変換開始時刻になったときその動作を開始するとよい。受注管理の場合には、ユーザコード、受注商品コード、受注個数、等のデータを含むメール等の形式のデータが受信データ記憶手段に記憶される。外部形式のデータ中に、例えば、ユーザコードの位置を示すデータが含まれていれば、そのデータを検出して切り取り、ユーザコードの部分のみを抽出できる。このとき、ユーザコードやその他の必要なデータ以外の部分は自動的に切り捨てられるので、不正なデータの取り込みが防止される。データ取り込みの際に、そのデータのフォーマットも検査するようにすれば、偽装されたデータの取り込みも防止できる。受信データ形式変換手段7は、こうして必要データ項目を抽出して、例えば、カンマで区切ったテキストデータを生成する。このデータを受信処理データ記憶手段8に書き込む。

【0053】

受信データ記憶手段に記憶された全てのデータD2の変換処理が終了すると、図3のステップS5からステップS6に進み、データベースのアップデート処理を実行する。受信処理データ記憶手段8に記憶されたデータD3は、そのままデータベースへ追記される。このデータD3が上記のようなCSV形式のデータの場合には、データベースへそのまま取り込むことができ、受注管理に使用される。

【0054】

なお、上記の例では、受信データ形式変換手段7による外部形式のデータ4から内部形式のデータ5への変換処理を実行してから、続いて、この内部形式のデータ5のホストコンピュータ側のデータベースへの追加記憶処理を実行するようにした。しかしながら、これらの処理はシステムの運用の便宜のために、それぞれ独自に実行されればよい。但し、受信データ形式変換手段7による変換処理は、ある程度外部形式のデータが蓄積されたときや、サーバへのアクセスが集中していないタイミングを狙って実行されることが好ましい。

【0055】

サーバが受信データ記憶手段に受信データを書き込むのは、通常、1個のデータごとになる。しかし、受信データ形式変換手段は、変換処理を一括して実行する。一括して実行するというのは、1個のデータごとではなく、バッチ処理のように複数のデータをまとめて処理するという意味である。独自のタイミングで実行されるというのは、それぞれ起動制御が独立しているという意味である。例えば、受信データ形式変換手段の変換処理が終了すると自動的に、ホストコンピュータ側のデータベースへの追加記憶処理が開始するように、動作タイミングを制御してもかまわない。

【 0 0 5 6 】

受信データ形式変換手段7は、単なるサーバとホストコンピュータとの間のインタフェースではない。不正なデータが含まれているかも知れない外部形式のデータから必要なデータのみを抽出加工して、予め定めた安全な内部形式のデータに変換をする一方通行のフィルタとしての役割を持つ。図1に示したネットワーク1を通じてサーバ3が受信した外部形式のデータは、受信データ記憶手段6に書き込まれるが、ホストコンピュータ10はこの受信データ記憶手段6を直接アクセスしない。故に、ホストコンピュータ10が、ネットワーク1から不正なデータを取り込むのを防止できる。

【 0 0 5 7 】

なお、図1において、受信データ記憶手段6は、サーバ3とは別に独立して設けた記憶装置であっても良いし、サーバやホストコンピュータ10の内部に設けられた記憶装置の一部であってもよい。また、受信処理データ記憶手段8も、サーバやホストコンピュータ10とは別に独立して設けた記憶装置であっても良いし、ホストコンピュータの内部に設けられた記憶装置の一部であってもよい。受信データ形式変換手段7は、サーバ3上で動作するコンピュータプログラムであってもよいし、ホストコンピュータ20上で動作するコンピュータプログラムであってもよい。

【 0 0 5 8 】

さらに、受信データ記憶手段6は、サーバ3が受信した外部形式のデータの書き込みを許容しても、サーバ3によるあらゆるデータの読み出しを禁止すること

が好ましい。これは、例えば良く知られたオペレーティングシステムの機能により実現する。また、あるいは、後で説明するように、サーバ 3 が受信データ記憶手段 6 にメール形式でデータを転送するようにすればよい。これによりネットワーク 1 側から受信データ記憶手段 6 中のデータの読み出しがされるのを防止できる。また、受信処理データ記憶手段 8 は、ホストコンピュータ 10 による内部形式のデータの読み出しを許容しても、ホストコンピュータ 10 によるあらゆるデータの書き込みを禁止することが好ましい。

【 0 0 5 9 】

同様に、受信データ形式変換手段 7 の動作にも制限を設けることができる。即ち、受信データ記憶手段 6 は、受信データ形式変換手段 7 による外部形式のデータの読み出しを許容する一方、受信データ形式変換手段 7 によるあらゆるデータの書き込みを禁止する。受信処理データ記憶手段 8 は、受信データ形式変換手段 7 による内部形式のデータの書き込みを許容する一方、受信データ形式変換手段 7 によるあらゆるデータの読み出しを禁止する。以上のように、一方通行の障壁をいくつも設けておくことにより、ハッカーから内部システムを有効に保護することが可能になる。

【 0 0 6 0 】

〈送信処理〉

図 4 は、本発明を送信処理のためのシステムに利用した例を示すブロックである。

図 1 に示したシステムは、ネットワークを通じて受信したデータを安全にホストコンピュータの処理するデータベース中に取り込むためのものであった。これはホストコンピュータからデータをネットワークに向けて送信する場合にも応用できる。図 4 はこの例を示すもので、図 1 のシステムと対比するため、図中に図 1 のシステムを構成するブロックを破線で表示して区別した。

【 0 0 6 1 】

図 4 のシステムは、ホストコンピュータ 10 は、送信データ記憶手段 12 と、送信データ形式変換手段 13 と、送信処理データ記憶手段 14 とを備える。その他は図 1 のシステムと同様である。ホストコンピュータ 10 は、データベース記

憶部 9 を使用して、受注管理等を実行する。送信処理データ記憶手段 1 4 は、このホストコンピュータが生成してネットワークに送信される、内部形式のデータを記憶する記憶装置である。送信データ形式変換手段 1 3 は、送信処理データ記憶手段 1 4 に記憶された内部形式のデータを外部形式のデータに変換して、送信データ記憶手段 1 2 に記憶させる機能を持つ。これも、図 1 の例と同様に、コンピュータプログラム等により構成される。サーバ 3 は、送信データ記憶手段 1 2 に記憶された外部形式のデータをネットワークに対して送信する機能を持つ。外部形式のデータ内部形式のデータの内容や形式は図 1 の例と同様でよい。

【 0 0 6 2 】

このシステムでは、ホストコンピュータ 1 0 は、ネットワークを通じて送信すべきデータがあると、任意のタイミングでこれを内部形式のデータにして、送信処理データ記憶手段 1 4 に記憶させる。送信データ形式変換手段 1 3 は、例えば、ホストコンピュータにより、そのつど起動されて、送信処理データ記憶手段 1 4 から内部形式のデータを読み取って、外部形式のデータに変換した後、送信データ記憶手段 1 2 に書き込む。この動作は、図 1 のデータ受信の場合と異なり、ホストコンピュータからデータ送信の緊急性についての情報を取得できるから、その点を考慮して、そのタイミングを選定すればよい。

【 0 0 6 3 】

サーバも、データが送信データ記憶手段 1 2 に書き込まれた後、データ送信の緊急性を考慮してネットワークへの送信処理を行えば良い。ここで、この例でも、送信処理データ記憶手段 1 4 は、ホストコンピュータ 1 0 による内部形式のデータの書き込みを許容する一方、ホストコンピュータ 1 0 によるデータの読み出しを禁止するとよい。また、送信データ記憶手段 1 2 は、サーバ 3 が送信する外部形式のデータの読み出しを許容する一方、サーバ 3 によるデータの書き込みを禁止することが好ましい。

【 0 0 6 4 】

さらに、送信処理データ記憶手段 1 4 は、送信データ形式変換手段 1 3 による内部形式のデータの読み出しを許容する一方、送信データ形式変換手段 1 3 によるデータの書き込みを禁止することが好ましい。また、送信データ記憶手段 1 2

は、送信データ形式変換手段 1 3 による外部形式のデータの書き込みを許容する一方、送信データ形式変換手段 1 3 によるデータの読み出しを禁止することが好ましい。以上のようにして、データ送信の場合には、ホストコンピュータからネットワークへの一方通行の障壁をいくつも設けて、ハッカーによるデータの不正取得を防止することができる。

【 0 0 6 5 】

また、送信データ形式変換手段 1 3 による内部形式のデータから外部形式のデータへの変換処理は、ホストコンピュータ 1 0 による送信処理データ記憶手段 1 4 への内部形式のデータの記憶処理とは独立したタイミングで実行してよい。図 1 に示したようなデータ受信のためのシステムと、図 4 に示したようなデータ送信のためのシステムを兼ね備えたシステムは、データの送受信に対して非常に高い保護が可能になる。

このとき、図 4 に示した受信データ形式変換手段 7 による変換処理と、内部形式のデータのホストコンピュータ 1 0 側のデータベースへの追加記憶処理と、ホストコンピュータ 1 0 による送信処理データ記憶手段 1 4 へのデータの記憶処理と、送信データ形式変換手段 1 3 による変換処理とは、それぞれ独立したタイミングで実行されることが好ましい。

【 0 0 6 6 】

図 5 は、システムのセキュリティ機能をさらに強化したシステムのブロック図である。

通常、コンピュータの記憶装置については、特定の領域のみを読み出し可能にし、他の領域については読み出しも書き込みも禁止するといった制御が可能である。しかしながら、このような制御はソフトウェアにより行うため、ハッカーによる不正な手段による侵入を完全に防止するのは容易でない。例えば、図 1 のシステムに示した各機能ブロックを一台のコンピュータを用いて実現した場合には、受信データ記憶手段 6 と受信処理データ記憶手段 8 と送信データ記憶手段 1 2 と送信処理データ記憶手段 1 4 とは同一のメモリ上に割りつけられる場合がある。また、サーバ 3 とホストコンピュータ 1 0 とを LAN（ローカルエリアネットワーク）で直接接続して、記憶装置を共有することもできる。そのような場合、

ホストコンピュータ側で保護されるべき受信処理データ記憶手段 8 や送信処理データ記憶手段 1 4 に対する不正アクセスを完全に防ぐのは容易でない。そこで、この例では、サーバとホストコンピュータ側の間を、データの一定形式の転送のみが可能なメールシステムで接続した。

【 0 0 6 7 】

図のサーバ 3 は、メールクライアント 3 1、記憶装置 3 3、メールサーバ 3 2 を備える。また、メール転送部 4 0 は、メール受信部 4 1 とメール送信部 4 2 を備える。更に、データ変換部 5 0 は、受信データ記憶手段 6 と、受信データ形式変換手段 7 と、受信処理データ記憶手段 8 と、送信データ記憶手段 1 2 とを備える。この具体例では、上記メール転送部 4 0 の機能により、サーバ 3 とホストコンピュータ側のデータ転送形態を制限して、ホストコンピュータ側の保護を強化している。また、メール転送部 4 0 に加えて上記データ変換部 5 0 を設ければ、より一層システムのセキュリティを高めることができる。

【 0 0 6 8 】

メール転送部 4 0 のメール受信部 4 1 は、メール受信機能を持つ装置で、メール送信部 4 2 はメール送信機能を持つ装置である。このメール転送部 4 0 とサーバ 3 とは、メール送受信用のケーブル 4 3、4 4 のみで接続されていること望ましい。こうすれば、サーバ 3 とメール転送部 4 0 との間でのデータ転送は、一定のメール形式以外で行われることがない。例えば、このメールで転送されるデータをテキストデータに限るようにすれば、不正なコマンドやプログラムがサーバ 3 とメール転送部 4 0 との間で転送されることが無い。

【 0 0 6 9 】

以上のシステムは次のように動作する。

サーバ 3 の記憶装置 3 3 には、例えばインターネット等のネットワーク 1 を通じて商品を販売するためのホームページ等のウェブページデータが格納されている。メールクライアント 3 1 は、端末装置 2 のユーザ等からネットワークを通じて商品発注のためのデータを受信すると、これをメール形式でメール転送部 4 0 のメール受信部 4 1 に送信する。メール受信部 4 1 は、受信したメールを受信データ記憶手段 6 に記憶させる。

【 0 0 7 0 】

その後の処理は既に説明したとおりで、データ形式の変換を経て、データベース 9 にそのデータが取り込まれる。データ変換部 5 0 は、データの形式をデータベース形式に変換して直接データベース 9 に書き込むような手段で構成してもよい。

【 0 0 7 1 】

一方、受注があった場合には、ホストコンピュータが「受信しました」といったコメントや、出荷日等を含む納期情報を生成する。このコメントや情報は、送信データ記憶手段 1 2 に記憶される。メール送信部 4 2 は、このコメントや情報をメール形式のデータにしてメールサーバ 3 2 に送信する。メールサーバ 3 2 は、そのデータをネットワークに向けて送信する。

【 0 0 7 2 】

即ち、メールクライアント 3 1 は、メール受信部 4 1 にメール形式のデータを送信するが、逆方向にメールを受信する機能は持たない。メールサーバ 3 2 はメール送信部 4 2 からメールを受信するが逆方向にメールを送信する機能は持たない。サーバ 3 とメール転送部 4 0 との間はメールを転送専用の通信回線等で接続されることが好ましい。こうして、サーバ 3 とメール転送部 4 0 とは、ハードウェア上も別体で構成できる。通信回線は、よりセキュリティを高めるために、他のデータの侵入経路を持たないものであることが好ましい。またメール形式のデータであって、他の形式のデータを転送しないから、不正なコマンドやデータがホストコンピュータ側に取り込まれることが無い。従って、確実な一方通行のデータ転送路となる。これにより、高いセキュリティが要求されるシステムについて高い保護機能が発揮される。

【 0 0 7 3 】

図 6 は、メール転送を利用してセキュリティを強化した別のシステムのブロック図である。

この図の例では、システム 2 0 のウェブサーバ 5 1 がネットワーク 1 に接続されて、ネットワーク 1 との通信を行う。このウェブサーバ 5 1 はメールサーバ 5 2 と接続されている。メールサーバ 5 2 は、メール転送部 4 0 のメール受信部 4

1 とメール専用線 5 3 を介して接続されている。また、メールサーバ 5 2 は、メール転送部 4 0 のメール送信部 4 2 とメール専用線 5 4 を介して接続されている。この図のメール転送部 4 0 以下ホストコンピュータまでの部分は、図 5 と同一である。なお、メール転送部 4 0 が直接ホストコンピュータ 1 0 に接続されていても、また、メール転送部 4 0 がホストコンピュータ 1 0 の一部に組み込まれていても、このシステムは十分に高いセキュリティが確保できる。

【 0 0 7 4 】

上記メール専用線 5 3、5 4 は、メールサーバ 5 2 とメール転送部 4 0 との間のメール転送にのみ使用される。メール転送以外に使用しないので、限られたフォーマットのデータ以外を転送することが出来ない。従って、ネットワーク側からホストコンピュータ側への不法侵入が確実に阻止される。また、ホストコンピュータ側からネットワーク側へ不用意にデータが送り出されることが無い。なお専用線 5 3、5 4 は図のように上りと下りで別々のケーブルにより構成してもよいし、双方向転送が可能な 1 本のケーブルにより構成しても構わない。また、この具体例では、上記の説明の都合上、ネットワーク 1 からウェブサーバ 5 1 の方向にのみデータが転送されるように矢印を示したが、ネットワーク 1 とウェブサーバ 5 1 間は双方向のコミュニケーションをしてさしつかえない。

【 0 0 7 5 】

上記のシステムでは、端末装置 2 から商品発注のためのデータがネットワーク 1 に送信されると、ウェブサーバ 5 1 がこれを受信する。ウェブサーバ 5 1 は、受信したデータをメールサーバ 5 2 に送信する。メールサーバ 5 2 は、そのデータをメール形式で専用線 5 3 を介してメール受信部 4 1 に送信する。一方、ホストコンピュータ 1 0 から送信されるメールは、メール送信部 4 2 から専用線 5 4 を介してメールサーバ 5 2 に転送される。メールサーバ 5 2 は、自己のメール送信機能を使って、ネットワーク 1 を通じて端末装置 2 に向けて送信する。その他の部分は、これまで説明したものと同様のため、重複する説明を省略するが、このような、専用線 5 3、5 4 を使用したメール転送により、ネットワークからの内部システムの保護強化を図ることができる。

【 0 0 7 6 】

なお、各図に示した各機能ブロックは、それぞれ別々のプログラムモジュールにより構成してもよいし、一体化したプログラムモジュールにより構成してもよい。また、これらの機能ブロックの全部または一部を論理回路によるハードウェアで構成しても構わない。また、各プログラムモジュールは、既存のアプリケーションプログラムに組み込んで動作させてもよいし、独立のプログラムとして動作させてもよい。

【図面の簡単な説明】

【図 1】

本発明のシステムの具体例を示すブロック図である。

【図 2】

サーバが受信したデータが変換されて受信処理データ記憶手段に記憶されるまでの動作を説明する説明図である

【図 3】

サーバや受信処理データ記憶手段等の動作のフローチャートである。

【図 4】

本発明を送信処理のためのシステムに利用した例を示すブロックである。

【図 5】

セキュリティ機能をさらに強化したシステムのブロック図である。

【図 6】

メール送信を利用してセキュリティ機能を強化した別システムのブロック図である。

【符号の説明】

- 1 ネットワーク
- 2 端末装置
- 3 サーバ
- 4 外部形式のデータ
- 5 内部形式のデータ
- 6 受信データ記憶手段
- 7 受信データ形式変換手段

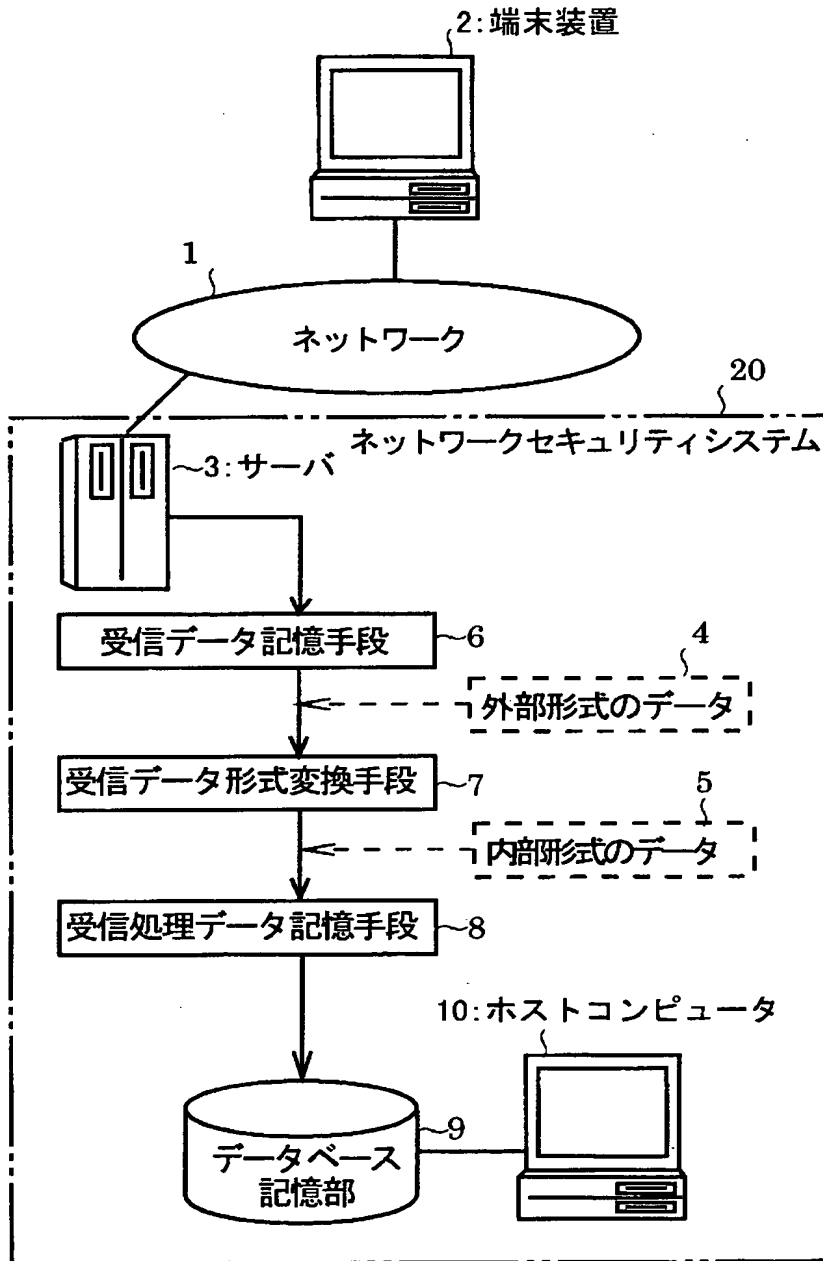
8 受信処理データ記憶手段

9 データベース記憶部

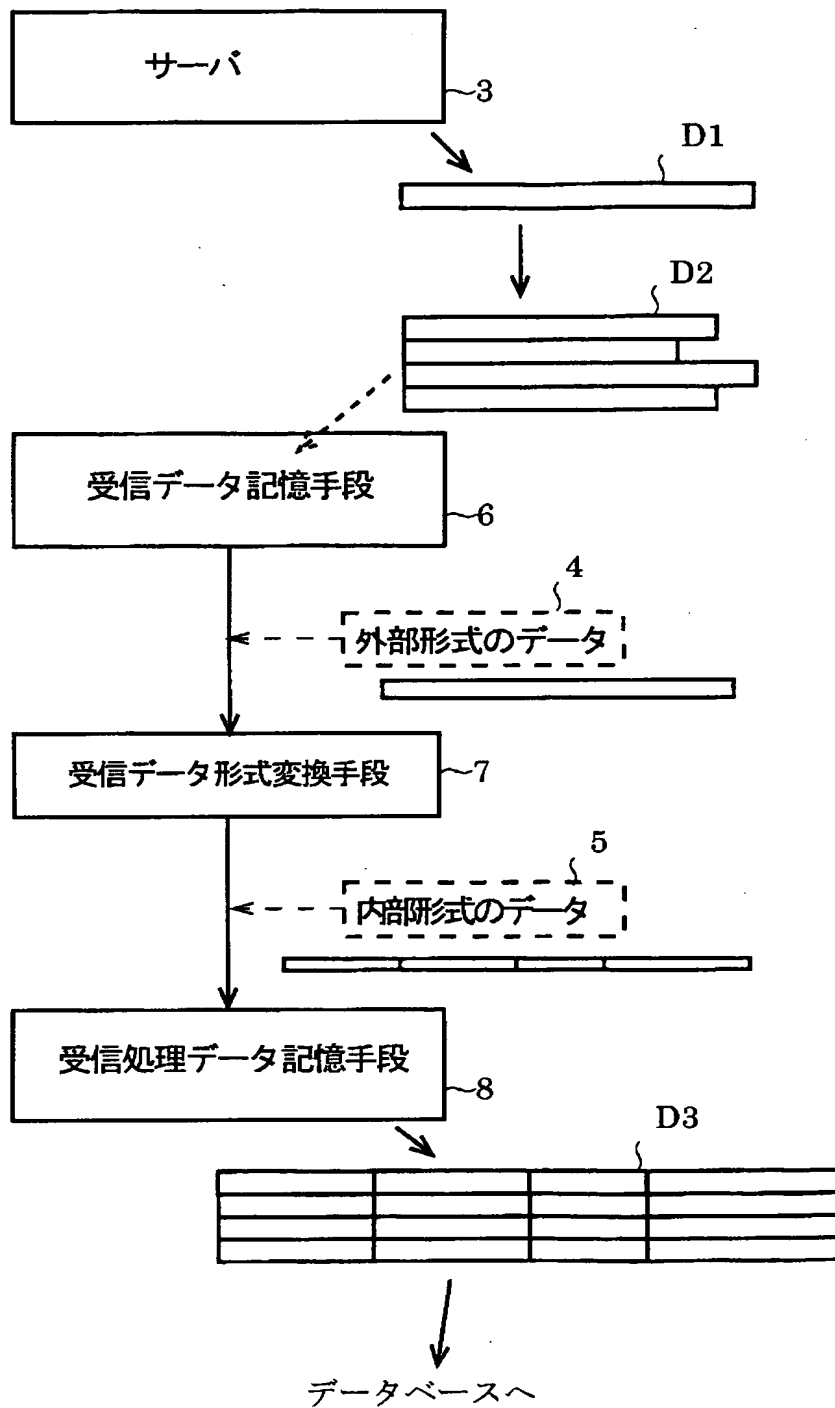
1 0 ホストコンピュータ

【書類名】 図面

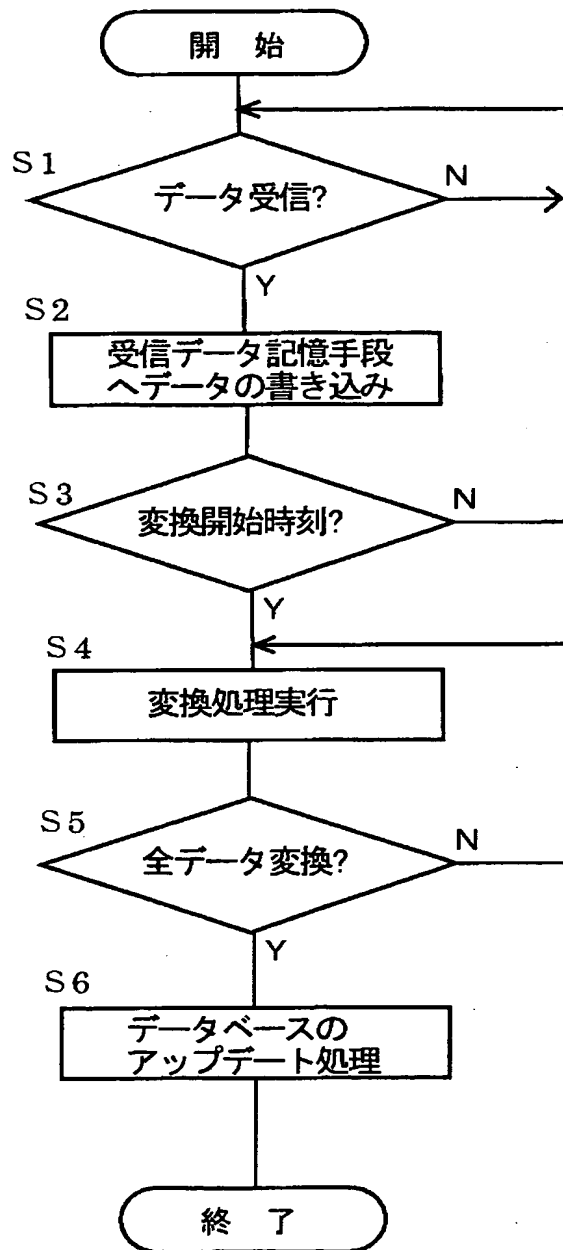
【図 1】



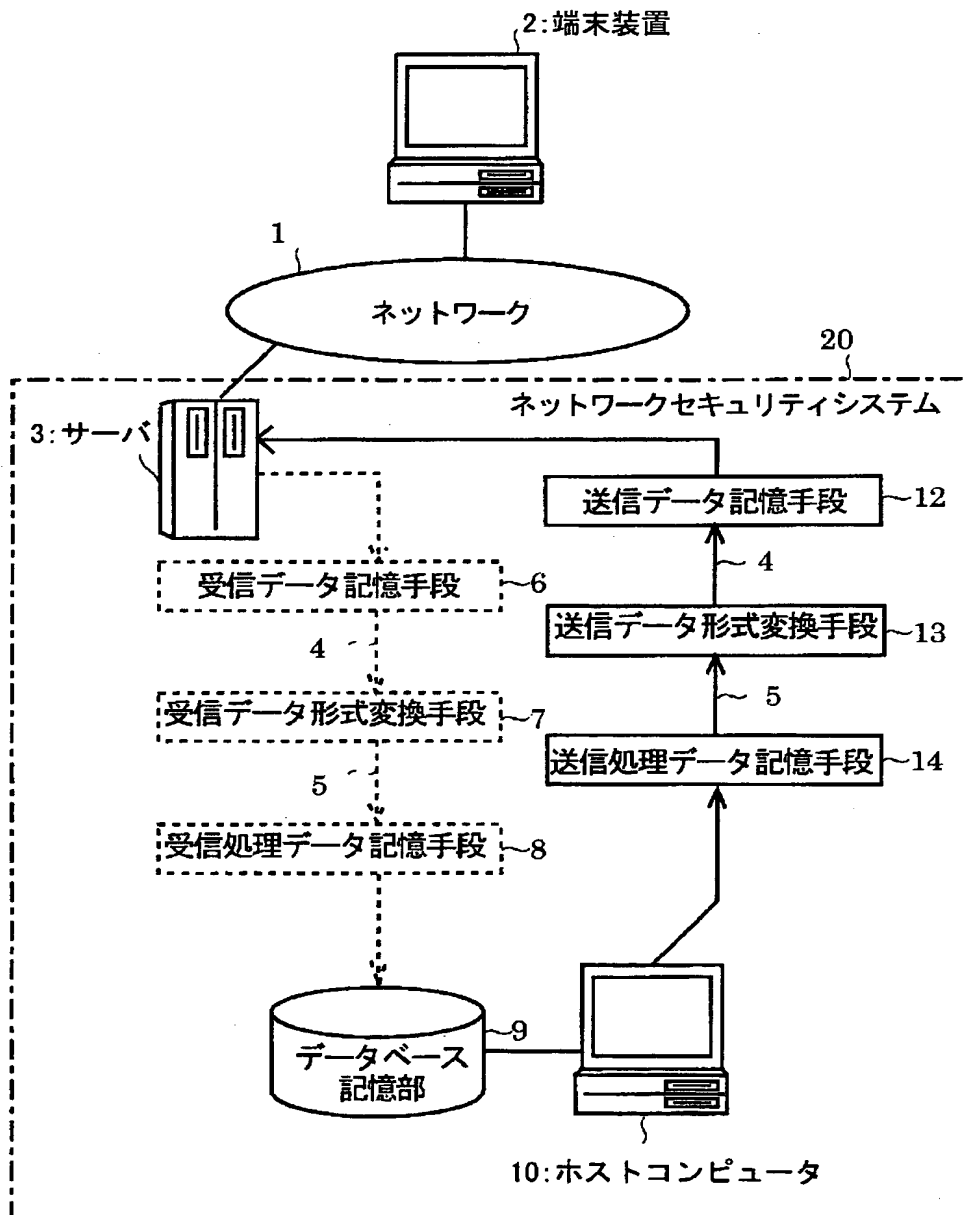
【図 2】



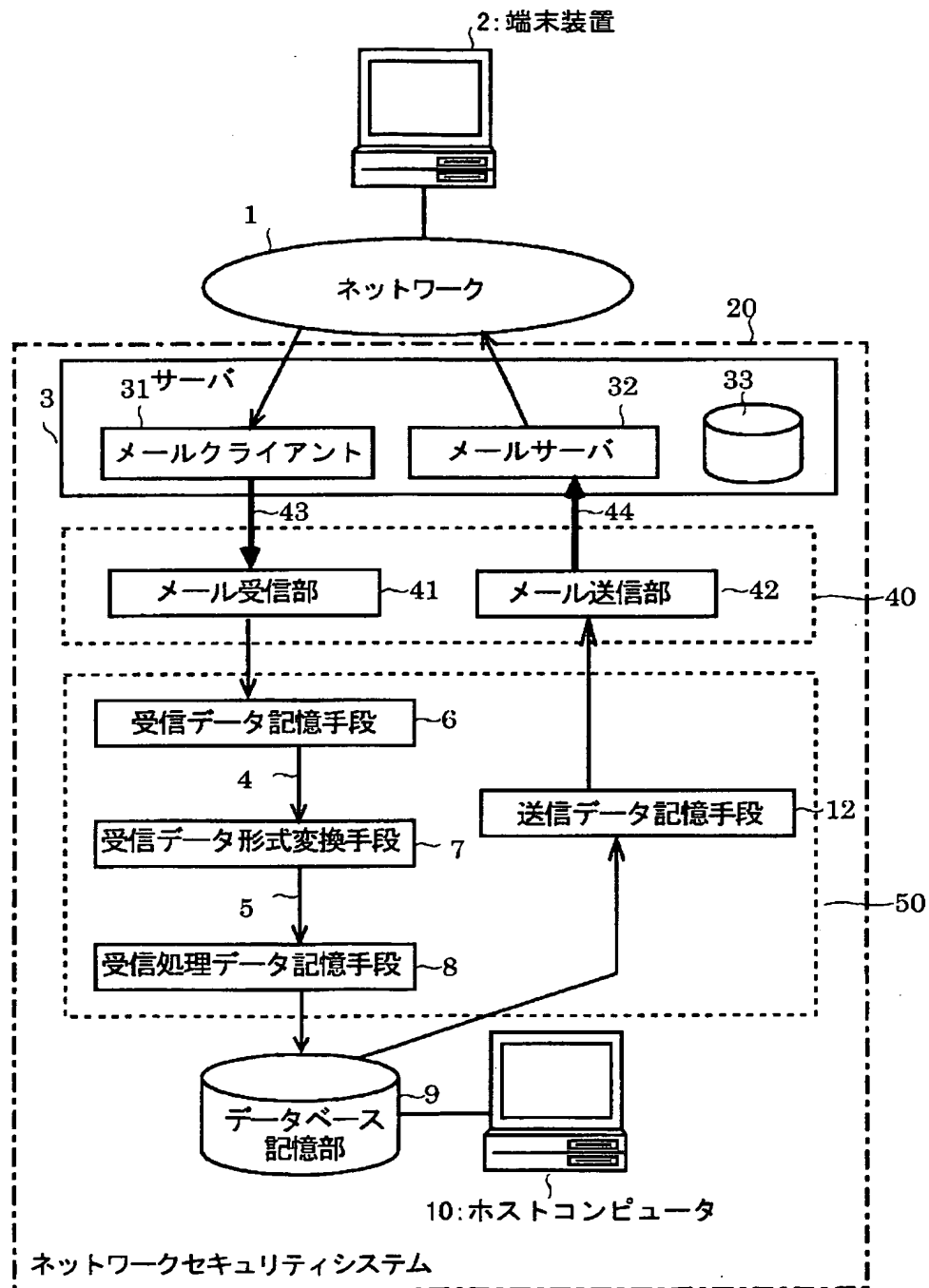
【図 3】



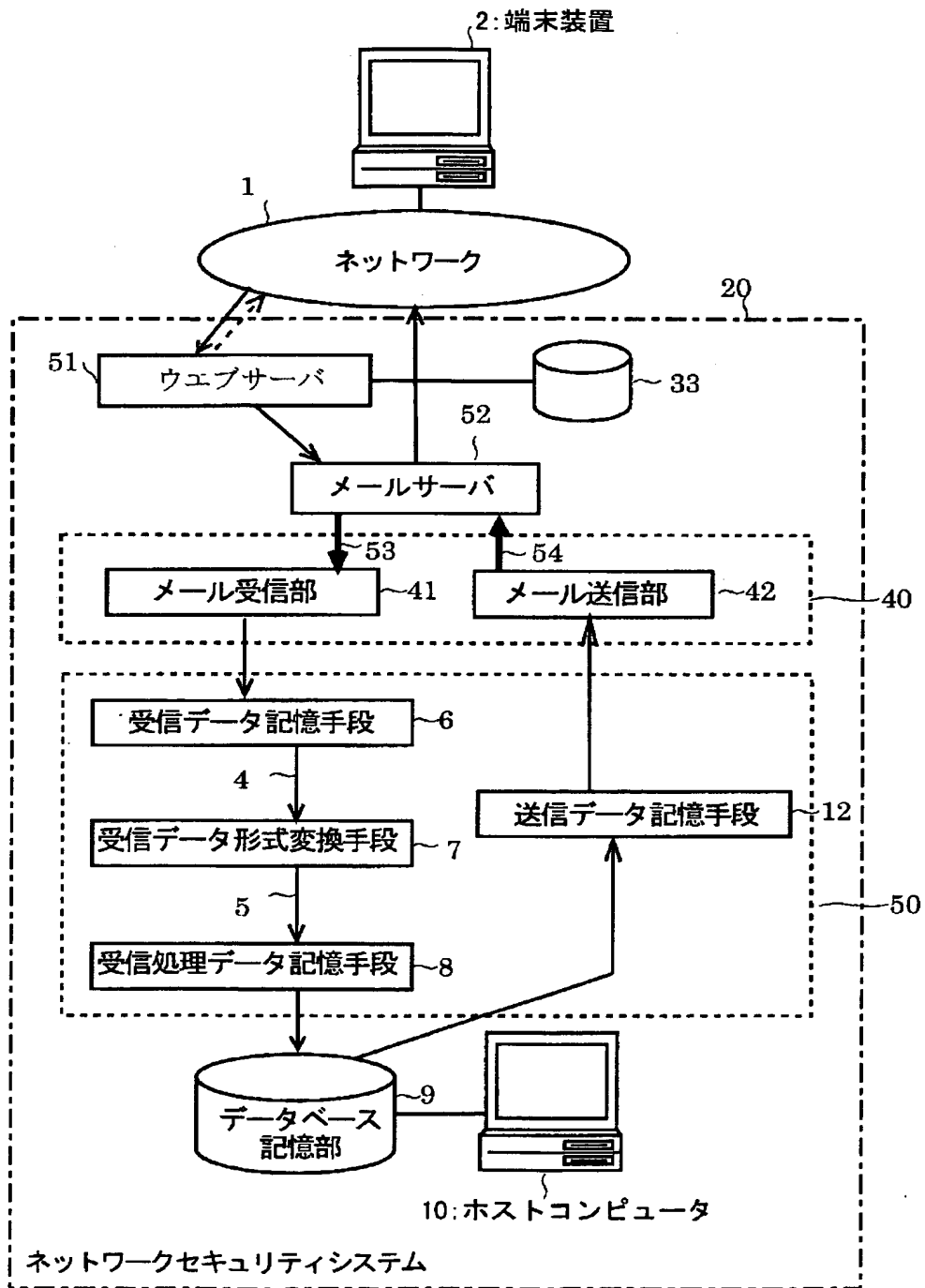
【図 4】



【図5】



【図 6】



【書類名】 要約書

【要約】

【解決手段】 ユーザから商品の受注をしたとき受注情報はネットワーク 1 を通じてサーバ 3 が受信する。受信データ記憶手段 6 はサーバが受信した外部形式のデータ 4 を記憶する。受信データ形式変換手段 7 は、受信データ記憶手段 6 に記憶された外部形式のデータ 4 を内部形式のデータ 5 に変換して、受信処理データ記憶手段 8 に記憶させる。ホストコンピュータ 1 0 は、受信処理データ記憶手段 8 に記憶された内部形式のデータ 5 を利用して受注管理をする。

【効果】 受信データ形式変換手段 7 が外部形式のデータ 4 を安全な内部形式のデータ 5 に変換することができるので、不正なデータを排除できる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002369]

1. 変更年月日 1990年 8月20日
[変更理由] 新規登録
住 所 東京都新宿区西新宿2丁目4番1号
氏 名 セイコーエプソン株式会社